IN THE CLAIMS:

Please amend the claims as follows. This listing of the claims will replace all prior versions of the claims in the application.

1. – 104. (Cancelled)

105. (New) A computer-implemented method comprising:

selecting an active program on a computer system as code under investigation, wherein at least some of the code associated with the selected active program is running in kernel mode; and

executing malicious code detection code (MCDC) on the computer system, wherein the MCDC includes a plurality of detection routines, wherein said executing includes:

applying the plurality of detection routines to the code under investigation, wherein said applying includes associating weights to the code under investigation in response to detections of a valid program or malicious code; and

determining whether the code under investigation is a valid program or malicious code as a function of the weights associated by the detection routines.

106. (New) The method of claim 105, wherein the code under investigation has access to other active programs executing on the computer system.

107. (New) The method of claim 105, further comprising:

selecting one or more additional active programs as code under investigation; and executing said MCDC with respect to said code under investigation.

108. (New) The method of claim 105, wherein the plurality of detection routines includes a plurality of valid program detection routines and a plurality of malicious code detection routines, wherein each of the plurality of detection routines individually associates weights to the code under investigation in response to detections of a valid program or malicious code.

109. (New) The method of claim 105, wherein the malicious code includes remote control software.

110. (New) The method of claim 105, wherein the malicious code includes a keystroke logger.

111. (New) The method of claim 105, wherein the malicious code includes spyware.

112. (New) The method of claim 105, wherein the malicious code includes a worm.

113. (New) The method of claim 105, wherein the malicious code includes a virus.

114. (New) The method of claim 105, wherein the malicious code includes monitoring software.

115. (New) A computer-implemented method comprising:

selecting a program currently running on a computer system as code under investigation, wherein said program is running in a manner that permits infection of said computer system; and

executing malicious code detection code (MCDC) on the computer system, wherein the MCDC includes a plurality of detection routines, wherein said executing includes:

applying the plurality of detection routines to the code under investigation, wherein said applying includes associating weights to the code under investigation in response to detections of a valid program or malicious code; and

determining whether the code under investigation is a valid program or malicious code as a function of the weights associated by the detection routines.

116. (New) The method of claim 115, wherein the code under investigation has access to other active programs executing on the computer system.

117. (New) The method of claim 115,wherein at least some of the code associated with the selected active program is running in kernel mode.

118. (New) The method of claim 115, further comprising:

selecting one or more additional active programs as code under investigation; and

executing said MCDC with respect to said code under investigation.

119. (New) The method of claim 115, wherein the plurality of detection routines includes a plurality of valid program detection routines and a plurality of malicious code detection routines, wherein each of the plurality of detection routines individually associates weights to the code under investigation in response to detections of a valid program or malicious code.

120. (New) The method of claim 115, wherein the malicious code includes a trojan horse.

121. (New) The method of claim 115, wherein the malicious code includes remote control software.

122. (New) The method of claim 115, wherein the malicious code includes a keystroke logger.

123. (New) The method of claim 115, wherein the malicious code includes spyware.

124. (New) The method of claim 115, wherein the malicious code includes a worm.

125. (New) The method of claim 115, wherein the malicious code includes a virus.

126. (New) The method of claim 115, wherein the malicious code includes monitoring software.

127.(New) A computer system comprising:

a processor; and

a memory storing program instructions executable by the processor to:

select a program currently running on a computer system as code under investigation, wherein said program is running in a manner that permits infection of said computer system; and

execute malicious code detection code (MCDC) on the computer system, wherein the MCDC includes a plurality of detection routines, including:

applying the plurality of detection routines to the code under investigation, wherein said applying includes associating weights to the code under investigation in response to detections of a valid program or malicious code; and

determining whether the code under investigation is a valid program or malicious code as a function of the weights associated by the detection routines.

128. (New) A computer-readable memory medium, including program instructions executable to:

select a program currently running on a computer system as code under investigation, wherein said program is running in a manner that permits infection of said computer system; and

execute malicious code detection code (MCDC) on the computer system, wherein the MCDC includes a plurality of detection routines, including:

applying the plurality of detection routines to the code under investigation, wherein said applying includes associating weights to the code under investigation in response to detections of a valid program or malicious code; and

determining whether the code under investigation is a valid program or malicious code as a function of the weights associated by the detection routines.